mkdir openssl\_eg

cd openssl\_eg/

Part 1

#Encryption

*Example 1.1 Check Open SSL Version Installed on Linux Machine*

openssl version

*Example 1.2 Check Open SSL commands*

openssl list -commands

*Example 1.3 Get the List of Encrypting Algorithms Available from Open SSL*

openssl list -cipher-commands

*Example 1.4 Creating a test message and encrypting it using AES-256-CBC algorithm & then Decrypting it using password*

touch message.txt; echo "This is my secret" > message.txt

*Note \* : Syntax*

*openssl <cmd> <cipher> -in <inputFile> -out <outputFile>*

*#Encryption*

openssl enc -aes-256-cbc -in message.txt -out enc-message-aes.bin -pbkdf2

*#Decryption*

openssl enc -aes-256-cbc -d -in enc-message-aes.bin -pbkdf2

*Example 1.5 Creating a test message and encrypting it using symmetric keys*

*Encrypt:*

openssl enc -in message.txt -out encrypted.dat -e -aes256 -k mysymmetrickey -pbkdf2

*Decrypt:*

openssl enc -in encrypted.dat -out outfile.txt -d -aes256 -k mysymmetrickey -pbkdf2

Part2

#Hashing

*Example 2 Example for HASHING using SHA1 Algorithm*

*\*\*Encrypting Message using Hashing, hash algorithm sha1*

openssl dgst -sha1 message.txt

Part 2

#Public Key Cryptography

\*\*Key Generation

\*\*Side A

*Example 3.1 Generating Private Key for USER A*

openssl genpkey -algorithm RSA -out privkey-A.pem

*Example 3.2 View your Private Key*

*Option 1:*

cat privkey-A.pem | less

*Option 2:*

openssl pkey -in privkey-A.pem -text | less

*Example 3.3 Generating Public Key from Private Key for USER A*

openssl pkey -in privkey-A.pem -out pubkey-A.pem -pubout

*Example 3.4 Generating Private Key & Public Key for USER B*

openssl genpkey -algorithm RSA -out privkey-B.pem

openssl pkey -in privkey-B.pem -out pubkey-B.pem -pubout

*Example 4 Example for Generating Digital Signatures and Signing a Test Message with it*

*\*\*Generating Digital Signature and Encrypting Message using private key of A*

openssl dgst -sha1 -sign privkey-A.pem -out signature.bin message.txt

*Example 5 Encrypting a message using Public Key of B (using public key from Example 3.4 for USER B)*

openssl pkeyutl -encrypt -in message.txt -pubin -inkey pubkey-B.pem -out ciphertext.bin

*Now you have*

1. Public and Private Keys for User A & User B in the folder
2. You Have a signature.bin from Example 4
3. Encrypted Text ciphertext.bin from Example 5

*\*\*Things that you will send to other side B by file transfer*

1. Public Key of A ie pubkey-A.pem

2. Signature ie signature.bin

3. Encrypted Text Message ie ciphertext.bin

\*\*Side B

*Example 6 Decrypting Message using Private Key of B*

openssl pkeyutl -decrypt -in ciphertext.bin -inkey privkey-B.pem -out received-message.txt

cat received-message.txt

*\*\*To verify whether it’s different with original file or not*

diff received-message.txt message.txt

*Example 7 Verify the Digital Signature*

openssl dgst -sha1 -verify pubkey-A.pem -signature signature.bin received-message.txt